

Entorno personal de aprendizaje:

Curso de Ciberseguridad: Seguridad en medios digitales



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

 **GOBIERNO
NACIONAL**

*Paraguay
de la gente*

Unidad 1. Control de Acceso - Credenciales

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Viceministerio de Tecnologías de la Información y Comunicación

Director General de Inclusión Digital y TIC en la Educación

Dirección General de Ciberseguridad y Protección a la Información

SEDE 1



Ministerio de
**TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN**

Dirección: Complejo Santos E2 - Gral. Santos 1170 c/ Concordia

Teléfono: (+595 21) 217 9000

Correo electrónico: comunicacion@mitic.gov.py

Mesa de entrada: sgeneral@mitic.gov.py

Asunción – Paraguay

Entorno personal de aprendizaje (PLE): Curso de Ciberseguridad: Seguridad en medios digitales

Todas las imágenes presentes en este material de apoyo educativo han sido reconocidas y, en todos los casos, son de uso libre. Todas las fuentes bibliográficas utilizadas en este material de apoyo educativo son citadas mediante el gestor de referencias bibliográficas Zotero, desarrollado por el Center for History and New Media de la Universidad George Mason, utilizando el estilo de la American Psychological Association Séptima Edición.

1. Autenticación

1.1. ¿Qué es la Autenticación?

La autenticación es el acto o proceso para el establecimiento o confirmación de algo (o alguien) como real, verificando su identidad.

El método de autenticación más utilizado en las plataformas en internet es, por lejos, el sistema basado en usuario y contraseña.



Desde hace varios años que los ataques a los sistemas de autenticación se han popularizado drásticamente: se han vuelto más frecuentes, más sofisticados, más fáciles de realizar.

Hoy en día, un atacante con herramientas de nivel intermedio es capaz de procesar 350 mil millones de contraseñas por segundo. Teniendo en cuenta esto, podemos calcular el tiempo teórico que tardaría para romper una contraseña de unas determinadas características:

	Números	Minúsculas	Minúsculas + números	Minúsculas + Mayúsculas + números
6 caracteres	<0,003 milisegundos	< 1 milisegundos	6 milisegundos	0,16 segundos
8 caracteres	0,3 milisegundos	0,6 segundos	8 segundos	10 minutos
10 caracteres	0,3 segundos	6,7 minutos	3 horas	1 mes
12 caracteres	3 segundos	3 días	5 meses	296 años

Unidad 1.

Control de Acceso - Credenciales

Además, pueden ser combinados varios tipos de ataques que pueden comprometer todo tipo de contraseñas en tiempos cada vez menores.



Es por eso que deben tomarse una serie de medidas de seguridad adicionales de modo a reducir el riesgo de que un atacante logre obtener acceso a nuestras cuentas.

2. Contraseñas

2.1. Buenas Prácticas de Contraseñas

Teniendo en cuenta lo fácil que es para un atacante romper una contraseña, es fundamental tomar una serie de medidas de seguridad adicionales de modo a reducir el riesgo de que un atacante logre obtener acceso a nuestras cuentas.



Unidad 1.

Control de Acceso - Credenciales

Las medidas son las siguientes:

- a)** Utilice contraseñas robustas: longitud mínima de 10-12 caracteres; combinación de letras, números, caracteres, etc.; use “frases” de seguridad en vez de palabras; evite palabras de diccionario, etc. En la sección “Contraseñas robustas” se profundizará acerca de las técnicas que pueden ser utilizadas para determinar si una contraseña es segura o no.
- b)** No utilice la misma contraseña para todo: Los ciberdelincuentes roban las contraseñas de los sitios web que cuentan con muy poca seguridad y, a continuación, intentan usar esas contraseñas y nombres de usuario en entornos más seguros, como sitios web de bancos.
- c)** Cambie sus contraseñas con regularidad: Establezca un recordatorio automático para cambiar las contraseñas de sus sitios web de correo electrónico, banca y tarjetas de crédito cada tres meses aproximadamente.
- d)** Variedad de Caracteres: Cuanto mayor sea la variedad de caracteres que contiene su contraseña, mejor. Use la totalidad del teclado, no solo las letras y los caracteres que usa o ve con mayor frecuencia.
- e)** No escribir ni reflejar la contraseña en un papel o documento donde quede constancia de la misma: no se deben guardar en documentos de texto dentro del propio ordenador o dispositivo (ej: no guardar las contraseñas de las tarjetas de débito/crédito en el móvil o las contraseñas de los correos en documentos de texto dentro del ordenador).
- f)** No compartir la contraseña: No enviar nunca la contraseña por correo electrónico o en un SMS. Tampoco se debe facilitar ni mencionar en una conversación o comunicación de cualquier tipo.
- g)** Nunca introducir una contraseña en un sitio o programa del cual no tengamos la certeza absoluta de que es legítimo. Existen diversos tipos de ataque, tales como los de ingeniería social (phishing u otras variantes) en los que la contraseña queda expuesta ante un atacante, por más robusta que sea. En la sección “Ingeniería social” se abordará con mayor detalle este tipo de ataques y como reconocerlos.
- h)** No escribir las contraseñas en ordenadores de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.).

Unidad 1.

Control de Acceso - Credenciales

- i) Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes e incluso por los administradores de sistemas.
- j) No utilizar herramientas online para crear contraseñas ni para encriptarlas/codificarlas. Muchas de estas herramientas almacenan estas contraseñas de modo a ampliar su base de datos de contraseñas conocidas.

2.2. Contraseñas Robustas



Antiguamente, la mayoría de los expertos de tecnología afirmaban que una contraseña robusta constaba de una combinación de al menos 8 caracteres.

Sin embargo, la creciente industria del “password cracking” ha obligado a rever esa definición, ya que hoy en día los 8 caracteres han dejado de ser suficientes, como vimos en la primera sección del módulo. Una contraseña robusta debe cumplir, en simultáneo, con las siguientes características:

- a) **Combinación de tipos de caracteres:** Es importante utilizar distintos tipos de caracteres: minúsculas, mayúsculas, números, caracteres especiales como: *#\$%&=?| u otros que fueran permitidos.
- b) **Frases:** Se pueden usar frases como contraseñas, estas pueden representar algo que tenga algún sentido para uno mismo pero que no fuera evidente para los demás. Lo ideal es que la misma no guarde relación con información personal (apodos, preferencias conocidas, etc.). Es aconsejable transformar dicha frase para convertirla en una combinación de letras mayúsculas y minúsculas, números y/o símbolos.

Unidad 1.

Control de Acceso - Credenciales

- c) **Evitar palabras de diccionario:** Al tratarse de palabras conocidas, es altamente probable que la misma se encuentre en alguna lista de palabras que los atacantes usan para sus ataques; a estas listas se le conoce como “diccionario”. Existen diccionarios con miles de millones de palabras, que incluyen casi todas las palabras y nombres que se nos pudieran ocurrir, incluidas combinaciones frecuentemente utilizadas como: admin, 12345, qwerty, asdfg, password, etc.

Curiosidad: Existen empresas que todos los años realizan un análisis de las contraseñas más utilizadas, obtenidas de fugas de información y/o hackeos. Mira [la lista de contraseñas más comunes](#).

Clave simple

Perro26!



Cambiamos algunas letras por números

P3rr026!



Jugamos con las mayúsculas para no crear patrones

P3rR026!



Por último, de igual modo movemos los números del final para romper el patrón

2P3rR06!

Clave robusta

2P3rR06!

3. Autenticación

3.1. Autenticación de Doble Factor (A2F)

La autenticación de doble factor trata de una medida de seguridad adicional que complementa la autenticación tradicional en los servicios. En otras palabras, además de requerir un nombre de usuario y contraseña, solicita el ingreso de un segundo factor de autenticación, como, por ejemplo, un código de seguridad. Generalmente, este código se genera en un dispositivo del usuario como un teléfono celular o token. Luego, la persona debe ingresarlo para poder validarse en el sistema.

Un sistema de doble autenticación es aquel que utiliza dos de los tres factores de autenticación que existen para validar al usuario. Estos factores pueden ser:

- ✓ Algo que el usuario sabe (conocimiento), como una contraseña.
- ✓ Algo que el usuario tiene (posesión), como un teléfono o token que le permite recibir un código de seguridad.
- ✓ Algo que el usuario es (inerencia), o sea, una característica intrínseca del ser humano como huellas dactilares, iris, etc.

Usuario + Contraseña + CÓDIGO DE SEGURIDAD



Por lo general, los sistemas de doble autenticación suelen utilizar los factores conocimiento (nombre de usuario y contraseña) y posesión (teléfono o token) para recibir código de seguridad. Hoy en día, la implementación mediante el teléfono es una de las más populares, ya que casi todo el mundo posee un smartphone.

Unidad 1.

Control de Acceso - Credenciales

Con este modelo de autenticación, si un atacante ha logrado obtener el usuario y contraseña de alguna manera, aun así, no podrá iniciar sesión debido a que no tendrá forma de obtener el código de seguridad ya que no posee el dispositivo del usuario.

La mayoría de los servicios como Google, Twitter, Outlook, etc. ofrecen esta característica de forma opcional para que cada usuario pueda activarlo. Es importante destacar que este tipo de protección no viene configurada por defecto, por lo tanto, el usuario deberá modificar algunos parámetros para activarla.

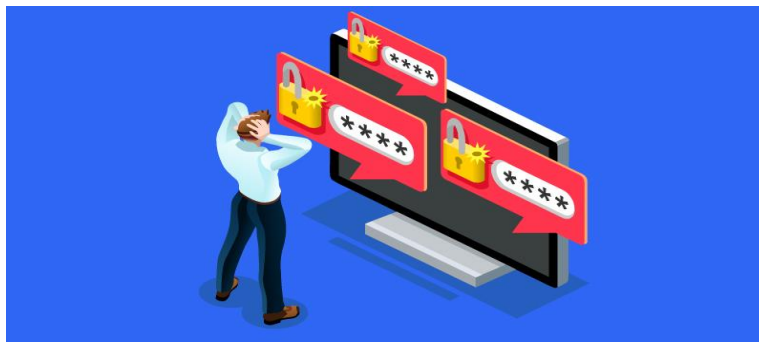
Además, los sitios web o blog basados en CMS como Wordpress, Joomla u otros CMS populares, cuentan con plugins que pueden ser integrados fácilmente para brindar una capa adicional de seguridad al sitio web.

A continuación, se despliega la configuración de activación de autenticación A2F de las aplicaciones más conocidas:

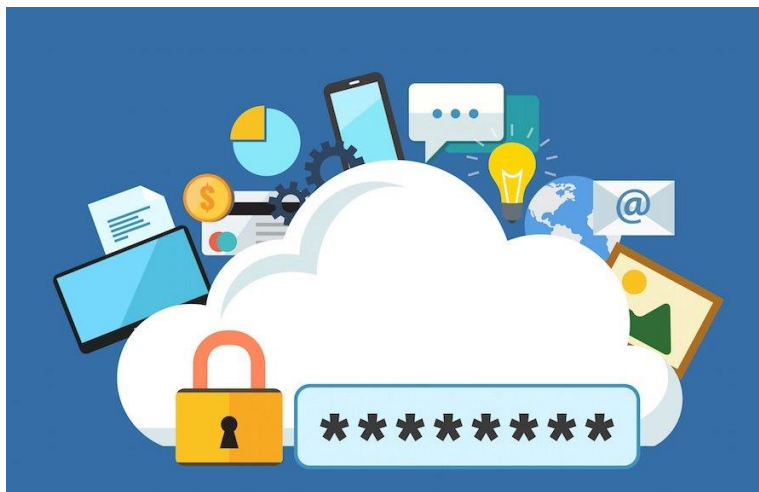
- [Como activar autenticación A2F Google](#)
- [Como activar autenticación A2F Facebook](#)
- [Como activar autenticación A2F Instagram](#)
- [Como activar autenticación A2F Twitter](#)
- [Como activar autenticación A2F Amazon](#)
- [Como activar autenticación A2F LinkedIn](#)
- [Como activar autenticación A2F Outlook](#)

4. Gestores de Contraseñas

Entre las recomendaciones para proteger las contraseñas, se ha mencionado la importancia de elegir contraseñas largas, diferentes para cada servicio y cambiarlas regularmente. Sin embargo, no es fácil recordar todas estas contraseñas, por lo que nos dificulta nuestra vida cotidiana.



Por esta razón se han desarrollado soluciones como los **gestores de contraseñas**. Son programas o aplicaciones que se utilizan para almacenar una gran cantidad de conjuntos de usuario-contraseña. La base de datos donde se guarda esta información está cifrada mediante una única clave (contraseña maestra o *master password*), de forma que el usuario sólo tenga que memorizar una clave para acceder a todas las demás. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente.



Unidad 1.

Control de Acceso - Credenciales

4.1. Tipos de Gestores

Es fundamental que la contraseña maestra sea lo suficientemente compleja para que sea difícil de romper, ya que, si un atacante consiguiera conocer la contraseña maestra y acceder a la base de datos del programa, ganaría acceso a todas nuestras claves.

Por eso, también es importante elegir un gestor de contraseñas que ofrezca autenticación de doble factor, además de otros mecanismos de seguridad que protejan nuestras contraseñas. Existen gestores de contraseñas que almacenan los datos de forma local, en el ordenador, y también existen otros que almacenan los datos online, en la nube. La mayoría de los navegadores también implementa funciones de almacenamiento de contraseñas básicas.

A continuación, presentamos algunos gestores de contraseñas más conocidos:

- LastPass: una herramienta gratuita basada en web, de código abierto, que se integra al navegador, por lo que puede ser utilizado en Windows, Mac, Linux y móviles.
www.lastpass.com
- Dashlane: otra herramienta basada en web.
<https://www.dashlane.com/es/passwordmanager>
- 1Password: disponible para varios sistemas operativos.
<https://agilebits.com/onepassword>
- KeePassX: una herramienta gratuita, de código abierto, disponible para varios sistemas operativos. <http://www.keepassx.org>
- KeePass: una herramienta gratuita de código abierta, para Windows. Es el antecesor de KeePassX. <http://keepass.info>

Muchas soluciones de antivirus incorporan funciones de administración de contraseñas, como, por ejemplo:

- Norton Identity Safe.
- Kaspersky Password Manager.

Unidad 1.
Control de Acceso - Credenciales

- Avast Easy Pass.
- McAfee LiveSafe.

Debido a que la seguridad de las contraseñas almacenadas dependerá de una única contraseña maestra, esto puede constituir un punto único de fallo. Por eso siempre es recomendable combinar los gestores de contraseñas con otros mecanismos de seguridad. Un ejemplo puede ser dejar las cuentas importantes (correo, bancos) con contraseñas seguras que no se guarden en el gestor y protegidas con autenticación en dos pasos, y utilizar el gestor para cuentas menos sensibles tales como foros, sitios de descarga, etc.